

REMARKS

The Examiner rejects claims 53-67 under 35 U.S.C. §102 as anticipated by Wu.

Claim 53 recites a method for authenticating a service computer with connection to a printing or copying system to be serviced. Claim 53 further recites the authentication server providing key data to the service computer defining access rights of the service computer. Claim 53 then recites transmitting authentication information with aid of this key data defining access rights to the printer. Claim 53 then recites that the printer control unit verifies the authenticity of the service computer based on this key data, and the system control unit checks the access rights, and if access is authorized, servicing the printing or copying system with the service computer.

At page 2 of the Examiner's response in paragraph 3 the Examiner contends that Wu teaches that the receiver in Figure 5 of Wu together with an associated "hardware device" controls the printing of the printer in Figure 5 of Wu, and therefore is somehow "servicing" the printer. But this argument fails to address the above quoted specific language of claim 53.

In Wu Figure 5, the sender sends a document to the trusted server. Before this, however, in a preregistration process, the receiver requests registration from the trusted server. The trusted server then sends back a registration identity to the receiver. The identity indicates that the receiver can receive controlled documents for printing by a printer which receives the controlled documents from the receiver. When the receiver is ready to send a controlled document to the printer, it requests, using its registration identify, the document from the trusted server. The trusted server then checks whether the receiver is authorized to receive that controlled

document. If it is, the document is then sent to the receiver (or the receiver together with a hardware device noted by the Examiner) and then sends the document to the printer. Alternatively, the hardware device may be part of the printer.

But a printer control unit in Figure 5 of Wu never checks access key data to see whether or not the receiver as a service computer is authorized to access the printer for servicing. Therefore Wu can never suggest the last paragraph of claim 53 reciting that a system control unit of the printer checks the access rights of the service computer defined by the key data before access to the printer is authorized for servicing the printer. This prevents an unauthorized service computer from gaining access to the printer. This concept is nowhere suggested in Wu. Significantly, Wu teaches away from the invention because in Wu the recipient computer always has access to the printer (with or without a hardware device).

For this last paragraph of claim 53 the Examiner first relies on page 2 paragraph 32 “usage control” and paragraph 35 “sender may be the one who authorizes the document”, and paragraph 47. Paragraph 32 is part of the trusted document structure including usage control and audit trail. But this is not a disclosure of the printer control unit checking access by a service computer. Paragraph 37 only deals with authentication of the sender and the recipient having nothing to do with the printer control unit checking by a service computer. Paragraph 47 talks about comparing a hash result before printing is authorized by the server. This has nothing to do with checking by a printer control unit whether access by a service computer should be allowed.

The Examiner further relies on page 3, paragraphs 54, 57 and 58. Paragraph 54 talks about issuing a license for the recipient to print the document. This has nothing to do with a printer control unit checking access by a service computer.

Paragraph 57 deals with print controls and whether or not a license is required for the printing. This has nothing to do with the printer control unit checking access by a service computer. Paragraph 58 talks about the document being sent by the recipient to a customer of the recipient or a secure hardware device controls the sending of the electronic document. Again there is no disclosure of a printer control unit checking access to the printer by a service computer.

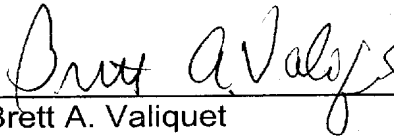
Next the Examiner relies on page 4 paragraphs 89-91, 95. But this only talks about the sender sending a secure document with no disclosure of a printer control unit checking access rights by a service computer to the printer. Finally the Examiner cites page 6, paragraph 155 which talks about the recipient submitting a request to print an authenticated document. Here, the server system verifies the document and sends the document to the recipient. Again there is no disclosure of a printer control unit checking access rights of the service computer before allowing servicing of the printer.

The following is also noted. In Wu paragraphs 0239 to 0326, always an authentication via a user name and a password takes place. Depending on the procedure, print data are indeed encoded with a session key. However, paragraph 0112 mentioned by the Examiner merely discloses this procedure for sending of a document 0109. However, the authentication of a service computer at a printer is not known from Wu. Rather, a direct access by the client to the printer does not take place, since in Wu, merely the "receiver" has access to the printer but not the sender (see Figs. 5, 9, 13, 17, 23).

In view of the above, reconsideration is respectfully requested and allowance of all claims 53-67 is requested.

The Commissioner is hereby authorized to charge any additional fees which may be required, or to credit any overpayment to account No. 501519.

Respectfully submitted,



(Reg.No.27,841)

Brett A. Valiquet
Schiff Hardin LLP
Patent Department
Suite 6600
Chicago, Illinois 60606
Telephone: (312) 258-5786
Attorneys for Applicants.
CUSTOMER NO. 26574

CH2\8383684.1